Appendix H
Classification

H.1 Overview

Throughout U.S. history, national defense has required that certain information be maintained in confidence in order to protect U.S. citizens, democratic institutions, homeland security, and interactions with foreign nations. Protecting information critical to the nation's security remains a priority.

The United States has devised its own classification system for safeguarding documents and other media, marking them, and granting access and clearance to obtain or view those documents. This appendix provides a classification reference for general issues and issues related to nuclear matters. This includes a discussion of: information classification, classification authorities, security clearances, accessing classified information, marking classified documents, and For Official Use Only (FOUO)/Official Use Only (OUO) and Unclassified Controlled Nuclear Information (UCNI).

H.2 Information Classification

There are two categories of classified information: national security information (NSI) and atomic energy (nuclear) information.

H.2.1 National Security Information

National security information is protected by Executive Order (EO) 13526. EO 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information. EO 13526 states that national security information may be classified at one of the following three levels:

- *Top Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *exceptionally grave damage* to the national security that the original classification authority is able to identify or describe.
- *Secret* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *serious damage* to the national security that the original classification authority is able to identify or describe.
- *Confidential* shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause *damage* to the national security that the original classification authority is able to identify or describe.

H.2.2 Atomic Energy (Nuclear) Information

Atomic energy (nuclear) information is protected by the *Atomic Energy Act (AEA) of 1954, as Amended*. The Department of Energy (DOE) implements the AEA requirements for classification and declassification of nuclear information via 10 CFR 1045. The AEA categorizes classified nuclear information as *Restricted Data (RD)*. RD is not subject to EO 13526.

- Restricted Data is all data concerning: design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy.

Classified nuclear information can be removed from the RD category pursuant to AEA sections 142d or 142e, and, after its removal, it is categorized respectively as *Formerly Restricted Data (FRD)* or *national security information (intelligence information)*.

- Formerly Restricted Data is jointly determined by the DOE and the Department of Defense (DoD) to relate primarily to the military utilization of atomic weapons and that can be adequately safeguarded as defense information (for example, weapon yield, deployment locations, weapons safety and storage, and stockpile quantities). Information characterized as FRD is not subject to EO 13526.

- Restricted Data information that is re-categorized as national security information refers to information that is jointly determined by the DOE and the Director of National Intelligence to be information that concerns the atomic energy programs of other nations and that can be adequately safeguarded as defense information (for example, foreign weapon yields). When removed from the RD category, this information is subject to EO 13526.

The DoD and the DOE have separate systems for granting access to atomic energy (nuclear) information.

The DoD System for Controlling Atomic Energy (Nuclear) Information

DoD policy governing access to and dissemination of RD is stated in DoD Directive 5210.2. The DoD categorizes RD information into Confidential RD, Secret RD, and Top Secret RD. Critical Nuclear Weapon Design Information (CNWDI) is a DoD access control caveat for a specific subset of Restricted Data. CNWDI information is Top Secret RD or Secret RD revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition, munition, or test device.[1] In addition, the DoD currently recognizes the designations of Sigma 14, Sigma 15, and Sigma 20, as defined by the DOE, as an additional subset of Restricted Data.

The DOE System for Controlling Atomic Energy (Nuclear) Information

The DOE policy of categorizing Restricted Data into defined subject areas is known as the *sigma system*. This categorization system separates RD information into common work groups to enforce need-to-know limitations. The sigma system applies strict security procedures to narrowly focused information areas. There are currently thirteen sigma categories, each of which contains a specific subset of RD information. Sigma categories 1-13 are defined by DOE Order 5610.2 Chg 1:

- Sigma 1: Information relating to the theory of operation (hydrodynamic and nuclear) or complete design of thermonuclear weapons or their unique components.
- Sigma 2: Information relating to the theory of operation or complete design of fission weapons or their unique components. This includes the high explosive system with its detonators and firing unit, pit system, and nuclear initiation system as they pertain to weapon design and theory.
- Sigma 3: Manufacturing and utilization information not comprehensively revealing the theory of operation or design of the physics package. Complete design and

[1] Sigma 1 and Sigma 2 generally, but not completely, equate to DoD CNWDI.

operation of nonnuclear components but only information as prescribed below for nuclear components. Utilization information necessary to support the stockpile to target sequence. Information includes:

a. General external weapon configuration, including size, weight, and shape;

b. Environmental behavior, fuzing, ballistics, yields, and effects;

c. Nuclear components or subassemblies that do not reveal theory of operation or significant design features;

d. Production and manufacturing techniques relating to nuclear components or subassemblies; and

e. Anticipated and actual strike operations.

- Sigma 4: Information inherent in preshot and postshot activities necessary in the testing of atomic weapons or devices. Specifically excluded are the theory of operation and the design of such items. Information includes:

  a. Logistics, administration, other agency participation;

  b. Special construction and equipment;

  c. Effects, safety; and

  d. Purpose of tests, general nature of nuclear explosive tested, including expected or actual yields and conclusions derived from tests not to include design features.

- Sigma 5: Production rate and/or stockpile quantities of nuclear weapons and their components.
- Sigma 6, 7, 8: These are no longer in use; they are subsumed by sigma 5.
- Sigma 9: General studies not directly related to the design or performance of specific weapons or weapon systems, e.g., reliability studies, fuzing studies, damage studies, aerodynamic studies, etc.
- Sigma 10: The chemistry, metallurgy, and processing of materials peculiar to the field of atomic weapons or nuclear explosive devices.
- Sigma 11: Information concerning inertial confinement fusion that reveals or is indicative of weapon data.
- Sigma 12: Complete theory of operation, complete design, or partial design information revealing either sensitive design features or how the energy conversion takes place for the nuclear energy converter, energy director, or other nuclear directed energy weapon systems or components outside the envelope of the nuclear source but within the envelope of the nuclear directed energy weapon.

- Sigma 13: Manufacturing and utilization information and output characteristics for nuclear energy converters, directors, or other nuclear directed energy weapon systems or components outside the envelope of the nuclear source, not comprehensively revealing the theory of operation, sensitive design features of the nuclear directed energy weapon, or how the energy conversion takes place. Information includes:
    a. General, external weapon configuration and weapon environmental behavior characteristics, yields, and effects.
    b. Component or subassembly design that does not reveal theory of operation or sensitive design features of nuclear directed energy weapons categorized as sigmas 1, 2, or 12.
    c. Production and manufacturing techniques for components or subassemblies of nuclear directed energy weapons that do not reveal information categorized as sigmas 1, 2, or 12.

Sigmas 14 and 15 define use control and are governed by DOE Manual 452.4-1A:

- Sigma 14: That category of sensitive information (including bypass scenarios) concerning the vulnerability of nuclear weapons to a deliberate unauthorized nuclear detonation.
- Sigma 15: That category of sensitive information concerning the design and function of nuclear weapon use control systems, features, and components. This includes use control for passive and active systems. It may include weapon design features not specifically part of a use control system. (Note: Not all use control design information is sigma 15.)
- Sigma 14 or 15 Access Authorization: Because of the extremely sensitive nature of sigma 14 and 15 information, all individuals who are granted access to sigma 14 and 15 must receive formal authorization by a DOE element or contractor organization with responsibility for sigma 14 or 15 nuclear weapon data (NWD).

Sigma 20 is a relatively new sigma category defined by DOE Order 457.1.

- Sigma 20: A specific category of nuclear weapon data that pertains to sensitive improvised nuclear device information.

H.3 Classifying Documents

In order to properly classify a document, an individual must have classification authority. There are two types of classification authority: original and derivative. A classifier is any

person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action.

H.3.1 Original Classification Authority

The authority to classify information originally may only be exercised by: the president and the vice president; agency heads and officials designated by the president; and U.S. government officials delegated the authority pursuant to EO 13526, Section 1.3., Paragraph (c). The original classification authority (OCA) also serves as the declassification authority or sets the date for automatic declassification. Within the DoD and the DOE, only appointed government officials can classify national security information. Further, only DOE officials can have original classification authority for RD information. In an exceptional case, when an employee or government contractor of an agency without classification authority originates information believed by that person to require classification, the information must be protected in a manner consistent with EO 13526 and the AEA. The agency must decide within 30 days whether to classify the information.

H.3.2 Derivative Classification Authority

According to EO 13526, those individuals who reproduce, extract, or summarize classified information, or who apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority. Individuals who apply derivative classification markings are required to observe and respect original classification decisions and carry forward the pertinent classification markings to any newly created documents. Individuals within both the DoD and the DOE can use derivative classification authority on national security information and RD and FRD information. These individuals are any employees or designated contractors with proper access to and training on classified materials.

H.4 Security Clearances

Both the DoD and the DOE issue personnel security clearances governing access of their employees and contractors to classified information.

H.4.1 Department of Defense Security Clearance Levels

The DoD defines a security clearance as an administrative determination by competent authority that a person is eligible under the standards of DoD 5200.2-R, *Personnel Security*

Program, for access to classified information. DoD clearances may be issued at the Top Secret, Secret, or Confidential level. These levels allow the individual holding the clearance, assuming that they have the proper "need to know"[2], to view information classified at those levels, as defined by EO 13526.

H.4.2 Department of Energy Security Clearance Levels

Corresponding to the information restrictions and guidelines in the *Atomic Energy Act of 1954*, the DOE established a security clearance system (implemented through DOE Order 472.1B) where:

- *L Access Authorization* is given to an individual whose duties require access to Confidential RD, Confidential/Secret FRD, or Confidential/Secret NSI.
- *Q Access Authorization* is given to an individual whose duties require access to Secret/Top Secret RD, Top Secret FRD, Top Secret NSI, or any category or level of classified matter designated as COMSEC, CRYPTO, or SCI.

H.4.3 Equating the Two Classification Systems

While it is not possible to directly correlate the two security clearance systems used by the DoD and the DOE, Figure H.1 shows the closest possible illustration of the overlap of atomic and national security information between the two departments.

DOE	DoD
L	C/S-NSI/FRD or C-RD
Q	Secret-RD
Q (w/ TS authority)	TS-RD
RD, FRD (Sigma System)	RD, FRD
Sigma 1 & 2	CNWDI
UCNI	UCNI

Figure H.1
Overlap of Atomic and National Security Information

H.5 Accessing Classified Information

There are two basic requirements to access classified information: appropriate clearance and "need to know." Both must be present for an individual to view classified information; rank, position, or clearance is not sufficient criteria from which to grant access. Personnel security clearance levels correspond to the security classifications. An individual may have

[2] *Need to know* is defined in DoD 5200.2-R as a determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, knowledge, or possession of classified information in order to perform tasks or services essential to the fulfillment of an official United States government program. Knowledge, possession of, or access to classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

a Confidential, Secret, Top Secret, or Top Secret/Sensitive Compartmented Information (SCI) clearance in the DoD; an individual may have L, Q, or Q with TS authority in the DOE. Each of these clearance levels also has an interim status, which allows the cleared person to view but not create or control documents at that level. Once the individual is given a final clearance, he/she is able to control documents for that level of classification. For example, within the DoD, individuals will not be afforded access to RD until they have been granted a final secret clearance. Most caveats are granted after individuals review a briefing explaining the nature of the material and sign forms. After completing this process, these individuals have the appropriate clearance to access the information. The process is commonly referred to as being "read-in" for a caveat.

"Need to know" is granted by the agency controlling the information and helps govern access to information. Security administrators verify an individual's eligibility for a certain clearance level, and then grant "need to know" caveats as needed.

To be given access to Top Secret or Secret RD/FRD or Q level information an individual must have a favorable single scope background investigation (SSBI). Access to Confidential RD/FRD or L level information requires a favorable national agency check with local agency and credit check (NACLC). In both instances, only the DOE, the DoD, the Nuclear Regulatory Commission (NRC), and the National Aeronautics and Space Administration (NASA) have the authority to grant RD/FRD access. To access CNWDI information, individuals require authorization and a briefing.

H.6 Marking Classified Documents

There are two types of documents that require classification markings: originally classified documents and derivatively classified documents.

H.6.1 Originally Classified Documents

EO 13526 requires certain essential markings on originally classified documents. DoD 5200.1-R stipulates marking requirements for classified documents. This section will explain each marking and how it is appropriately placed in a classified document. The essential markings are: portion marking, overall classification, "classified by" line, reason for classification, and "declassify on" line.

Portions can be paragraphs, charts, tables, pictures, illustrations, subjects, and titles. Before each portion a marking is placed in parentheses. (U) is used for Unclassified, (C) for Confidential, (S) for Secret, and (TS) for Top Secret. The subsequent paragraph underneath

also has its own classification marking. The classification of the portion is not affected by any of the information or markings of other portions within the same document.

After portion marking, the classifier must determine the overall classification of the document. The document is classified at the highest level of the portion markings contained within the document. The classification is centered in both the header and footer of the document. It is typed in all capital letters and in a font size large enough to be readily visible to the reader. This marking is noted on the front cover, the title page, the first page, and the outside of the back cover. Internal pages may be marked with the overall document classification or the highest classification level of the information contained on that page. The most common practice is to mark all internal pages with the overall document classification.

In the lower left-hand corner of the title page, the original classification authority is identified. Authority must be identified by name (or personal identifier) and position. If the agency of the original classifier is not readily apparent, then it must be placed below the "classified by" line.

The reason for classification designation is placed immediately below the "classified by" line. This line should contain a brief reference to the classification category and/or classification guidance. The number 1.4 may appear with corresponding letters, representing section 1.4 of EO 13526 and the classification categories it defines. The information being classified must relate to one of the following classification categories:

a. military plans, weapons systems, or operations;
b. foreign government information;
c. intelligence activities (including covert action), intelligence sources or methods, or cryptology;
d. foreign relations or foreign activities of the United States, including confidential sources;
e. scientific, technological, or economic matters relating to the national security;
f. United States government programs for safeguarding nuclear materials or facilities;
g. vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
h. the development, production, or use of weapons of mass destruction.

The final essential marking is the "declassify on" line. One of three rules listed below is used in determining how long material is to stay classified. All documents must have a declassification date or event entered onto the "declassify on" line. The original classifying authority determines the "declassify on" date of the document using the following guidelines:[3]

1. When possible, identify the date or event for declassification that corresponds to the lapse of the information's national security sensitivity. The date or event shall not exceed 10 years from the date of the original classification; or
2. When a specific date or event cannot be determined, identify the date that is 10 years from the date of the original classification; or
3. If the sensitivity of the information warrants protection beyond 10 years, then the original classification authority may assign a declassification date up to but no more than 25 years from the date of original classification.

H.6.2 Derivatively Classified Documents

Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form, information that is already classified and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or documents or a classification guide issued by an OCA. It is important to note that the DoD can only derivatively classify documents containing RD.

Derivative Classification Using a Single Source Document or Multiple Source Documents

When using a classified source document as the basis for derivative classification, the markings on the source document determine the markings to be applied to the derivative document. As with documents created by original classifiers, each derivative document must have portion markings and overall classification markings.

Derivatively classified documents are handled in much the same manner as originally classified documents except for two markings. In a document derived from a single source, portion markings, overall markings, and "Declassify on" lines all remain the same as the original document. In a document derived from multiple sources, before marking the document with the "Declassify on" line, it is necessary to determine which source document requires the longest period of classification. Once that has been determined,

[3] Whenever possible, the original classifying authority should select the declassification instruction that will result in the shortest duration of classification.

the derivative document should reflect the longest period of classification of any of the source documents.

In a derivatively classified document, the "Classified by" line identifies the name and position of the individual classifying the document. The name and position should be followed by the derivative classifier's agency and office of origin. In addition, a derivatively classified document includes a "Derived from" line. In a document derived from a single source, this is a brief description of the source document used to determine the classification of the information. Documents whose classifications are derived from multiple sources are created in the same manner as documents derived from a single classified source. Enter "Multiple Sources" on the "Derived from" line. On a separate sheet of paper, a list of all classification sources must be maintained and included as an attachment to the document. When classifying a document from a source document marked "Multiple Sources," do not mark the derived document with "Multiple Sources." Instead, in the "Derived from" line, identify the source document. In both cases, the "Reason" line, as reflected in a source document or classification guide, is not required to be transferred to a derivatively classified document.

Derivative Classification Using a Classification Guide

A classification guide is a document issued by an OCA that provides classification instructions. A classification guide describes the elements of information that must be protected and the level, reason, and duration of classification. When using a classification guide to determine classification, insert the name of the classification guide on the "Derived from" line. Portion markings are determined by the level of classification of the information as listed in the classification guide, and the overall marking is determined by the highest level of the portion markings contained within the document. Finally, the "Declassified on" line is determined by the classification duration instruction in the guide.

H.6.3 Marking Restricted Data and Formerly Restricted Data Documents

There is a special requirement for marking RD, FRD, and CNWDI documents. The front page of documents containing RD must include the following statement:

> RESTRICTED DATA
> This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

This may appear on the first page of the document and on a second cover page, placed immediately after the initial classified cover sheet. FRD material must contain the following statement on the front page of the document:

> FORMERLY RESTRICTED DATA
> Unauthorized disclosure subject to administrative
> and criminal sanctions. Handle as Restricted Data in
> foreign dissemination. Section 144b, AEA 1954.

Additionally, documents containing RD and FRD should have abbreviated markings ("RD" or "FRD") included with the classification portion marking (e.g., (S-RD) or (S-FRD)). Documents containing RD and CNWDI material must also contain the following statement in addition to the RD statement on the front page of the document:

> CNWDI
> Critical Nuclear Weapon Design Information.
> DoD Directive 5210.2 applies.

Additionally, CNWDI is marked with an "N" in separate parentheses following the portion marking (e.g., (S-RD)(N)).

Finally, when a document contains RD, FRD, and CNWDI, only the RD and CNWDI warning notices are affixed. No declassification instructions are used.

H.7 For Official Use Only and Unclassified Controlled Nuclear Information

For Official Use Only and Official Use Only are terms used by the DoD and the DOE, respectively, that can be applied to certain unclassified information. FOUO and OUO designations indicate the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other agency-authorized activities; and may be exempt from mandatory release under one of eight applicable Freedom of Information Act (FOIA) exemptions listed below:

1. Information that pertains solely to the internal rules and practices of the agency.
2. Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.

3. Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness.
4. Interagency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions, and recommendations.
5. Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
6. Records or information compiled for law enforcement purposes that: could reasonably be expected to interfere with law enforcement proceedings, would deprive an individual of a right to a fair trial or impartial adjudication, could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others, disclose the identity of a confidential source, disclose investigative techniques and procedures, or could reasonably be expected to endanger the life or physical safety of any individual.
7. Certain records of agencies responsible for supervision of financial institutions.
8. Geological and geophysical information concerning wells.

The DoD and the DOE also use the term Unclassified Controlled Nuclear Information. DoD defines UCNI as unclassified information pertaining to security measures (including plans, procedures, and equipment) for the physical protection of DoD special nuclear material, equipment, or facilities. While this information is not formally classified, it is restricted in its distribution. DoD UCNI policy is stated in DoDD 5210.83. The DOE uses the term UCNI in a broader manner than the DoD. Designating DoD information as UCNI is governed by 10 USC 128; designating DOE information as UCNI is governed by 42 USC 2168 et seq.

While protecting information critical to the nation's security is a priority, the U.S. government is also committed to open government through the accurate and accountable application of classification standards. An equally important priority is the assurance of routine, secure, and effective declassification. Strict adherence to the classification principles described above is extremely important to ensure the achievement of these goals while protecting the country's national security information.